Diagnosability of hybrid automata with measurement uncertainty

Maria D. Di Benedetto, Stefano Di Gennaro and Alessandro D'Innocenzo
Department of Electrical and Information Engineering, and Center of Excellence DEWS.
University of L'Aquila - Italy. E.mail: {*dibenede,digennar,adinnoce*}@*ing.univaq.it*

Abstract— **We propose a diagnosability notion that depends on two parameters denoted as (δ_d, δ_m) for the general class of transition systems where the observable output is given by discrete symbols and by the delay between the generation of two symbols. The first parameter specifies that if a trajectory (state execution) has visited the faulty set, this can be detected only using the external trajectory (observable output) within a delay upper-bounded by δ_d. The second parameter specifies the available precision δ_m when measuring time delays of the external trajectory. Given an approximate abstraction T_1 of a system T_2 with precision ε, we derive a relation between diagnosability properties of T_1 and T_2 with respect to the parameters $\delta_d, \delta_m, \varepsilon$. We apply our results to an electromagnetic valve system for cam-less engines.**

I. Introduction

The increase of functionality offered by control systems based on *embedded systems* requires more effort to verify the controlled system, as a malfunction can yield catastrophic results. Most of the plants of interest have continuous dynamics. Thus the controlled system has a mix of discrete and continuous dynamics. Systems characterized by discrete and continuous components in their dynamics are called hybrid systems [2]. Hybrid systems are an example of very general systems, whose great expressive power has to be paid by the lack of strong theoretical results and consequent difficulties in verifying the properties of a closed loop system. Formal verification (e.g. *model checking* [5]) of properties where the state space is semi–exhaustively searched are complicated by the very large dimensions of the state space. *Abstraction* is an important technique used to cope with this complexity problem. By abstraction, we create a system with smaller state space (even finite) that is equivalent to the original system. System equivalence is usually defined by the notions of language equivalence and bisimulation [3], [23]. These notions are very restrictive, since they require perfect equivalence of trajectories. Recently, approximate notions of system equivalence [16], [15], [17], [18], [19] were developed to relax the abstraction problem, where a metric is introduced to quantify the distance between the original system and the abstraction. Other results in approximation theory for timed systems can be found e.g. in [4], [13].

We discuss in this paper automatic verification of diagnosability properties for general class of transition systems using approximate abstraction methods. Diagnosability corresponds to failure detection in finite time, and has many applications in several fields, e.g. the detection of an error in an air traffic management procedure [6], [7], a failure in an automotive system [14], in a component of an industrial plant, or in a communication system [25]. Given a system, we say that a fault occurs if an execution visits a given *faulty* subset of the state space. A system is diagnosable if, within a finite time bound and only using the observable output of the plant, it is possible to detect that a fault has occurred. We consider the observable output only given by discrete output symbols (possibly unobservable) associated to the state transitions, and delay between the symbol generation.

Given a plant and a set of faulty states, an important problem often addressed in the literature is verifying automatically whether the system is diagnosable. For the class of discrete event systems (DESs), the diagnosability verification problem was treated in several papers by Feng Lin [20] and Lafortune [24], [27], [22]. The diagnosability verification problem was shown to belong to the complexity class *P*. In these papers, since the concept of time flow is not present in DESs, a plant is defined diagnosable if it is possible to detect a failure after a finite number of transitions since the fault has occurred, rather than after a time delay. For the class of timed automata, a definition of δ–diagnosability has been proposed by Tripakis [26]: a plant is δ-diagnosable if it is possible to detect a failure after a time delay bounded by $\delta \in \mathbb{N}$ since the fault has occurred. The diagnosability verification problem for timed automata was demonstrated to be in PSPACE. Diagnosability of hybrid systems was considered by Fourlas in [14], where a notion of diagnosability was proposed for input–output automata, diagnosability conditions were stated, but no complexity analysis was performed. In [21], a hybrid diagnosis problem was formulated, and qualitative techniques for the diagnosis of continuous time systems were proposed. In [28], a design procedure for a diagnosis system and a mode estimation algorithm for hybrid automata are presented. Given a hybrid automaton, we proposed in [8] a conservative abstraction procedure that allows to verify δ-diagnosability of the original system on a durational graph abstraction. Durational graphs are a subclass of timed automata, see [11] for more details). If the abstraction is δ-diagnosable, then the original system is δ-diagnosable. However, this approach has the following weak points: (1) it is not known how conservative the approximation is, and (2) if the abstraction is not δ–diagnosable, then nothing can be implied on the original system.

In this paper, we extend our previous results to tackle these problems. To address the first issue, we define a metric to measure how closely the observations of our abstraction match those of the original system, and relate it to the notion of approximate bisimulation relations [15]. To solve the second issue, we build upon the results in [11], where we proposed an algorithmic procedure to obtain a durational graph abstraction of a given hybrid automaton for any precision, and a δ–diagnosability polynomial verification algorithm for durational graphs. The proposed abstraction, however, is affected by an approximation error in the discrete transitions time duration that diverges to infinity as time goes to infinity. This error explosion introduces technical problems when formally relating diagnosability of the original system with respect to diagnosability of the abstraction. For this reason, we propose a more general diagnosability definition, which depends on two parameters (δ_d, δ_m). The first parameter specifies that if a trajectory has visited the faulty set, this can be detected only by using

This work was partially supported by European Commission under Project IST NoE HYCON contract n. 511368, and by STREP project n. TREN/07/FP6AE/S07.71574/037180 IFLY

the external trajectory within a delay upper-bounded by δ_d. The second parameter specifies the available precision δ_m when measuring time delays of the external trajectory. We propose necessary and sufficient conditions for this more general definition. The main contribution of the paper is formally relating the diagnosability of a general dynamical system and an ε bisimilar abstraction. This result is proven in the framework of transitions systems, and thus it applies to very general classes of dynamical systems. We use our result to verify diagnosability of a general hybrid automaton, on the durational graph abstraction we proposed in [11], and apply our theoretical investigation to an electromagnetic valve system for cam-less engines.

The paper is organized as follows. In Section II we introduce the basic definitions of transition systems and approximate bisimulation. In Section III the definition of diagnosability for transition systems is formalized, which generalizes the notion of diagnosability given in [8]. In Section IV, we formally relate diagnosability properties of two ε bisimilar transition systems. Then, we specialize the general result to verify diagnosability of hybrid automata on durational graph abstractions. In Section V we apply our verification procedure by abstraction to an electromagnetic valve system for cam-less engines. Some concluding remarks are offered in Section VI.

II. Basic definitions

We introduce the framework of metric transition systems [15], which enable us to model continuous and discrete dynamical systems:

Definition 1 (Metric transition system): A labeled metric transition system is a tuple $\mathcal{T} = (Q, Q_0, \Sigma, E, \Omega, \omega)$ that consists of a possibly infinite set Q of states; a possibly infinite set $Q_0 \subseteq Q$ of initial states; a possibly infinite set Σ of labels; a transition relation $E \subseteq Q \times \Sigma \times Q$; a possibly infinite set Ω; a map $\omega : Q \to \Omega$; metrics d_Σ, d_Ω on Σ and Ω.

In what follows, we write $q \overset{\sigma}{\to} q'$ to denote that $(q, \sigma, q') \in E$. We assume that the systems we consider are *non–blocking*, i.e. for all $q \in Q$ there exists at least an outgoing transition $q \overset{\sigma}{\to} q'$. We say that a transition system $\mathcal{T}$ is *deterministic*, if for all $q \in Q, \sigma \in \Sigma$ there exists at most a unique transition $q \overset{\sigma}{\to} q'$, and the set Q_0 contains a single element.

A *trajectory* of $\mathcal{T}$ is a finite or infinite sequence of transitions $\rho = \omega(q_0) \overset{\sigma_1}{\to} \omega(q_1) \cdots \overset{\sigma_{|\rho|}}{\to} \omega(q_{|\rho|})$, where $q_0 \in Q_0$ and $\forall i = 0 \cdots |\rho| - 1, q_i \overset{\sigma_{i+1}}{\to} q_{i+1}$. We define the language $\mathcal{L}$ as the set of all trajectories generated by $\mathcal{T}$.

To each trajectory $\rho = \omega(q_0) \overset{\sigma_1}{\to} \omega(q_1) \cdots \overset{\sigma_{|\rho|}}{\to} \omega(q_{|\rho|})$, we associate an *external trajectory* as a sequence $P(\rho) = \sigma_1, \cdots, \sigma_{|\rho|}$. We define the language $\mathcal{P}$ as the set of all external trajectories generated by $\mathcal{T}$.

Let $\mathcal{X}(\Sigma)$ be the set of all strings over Σ, and let $d_\mathcal{X}$ be a metric on $\mathcal{X}(\Sigma)$. Let $h_{\overrightarrow{\mathcal{X}}}$ and $h_\mathcal{X}$ denote the directed and undirected Hausdorff distance associated to a metric $d_\mathcal{X}$. Given $\mathcal{T}_1, \mathcal{T}_2$ and the corresponding languages $\mathcal{P}_1, \mathcal{P}_2$ subsets of $\mathcal{X}(\Sigma)$, we can define a language metric as the Hausdorff distance between two languages: $d_{\overrightarrow{\mathcal{P}}}(\mathcal{T}_1, \mathcal{T}_2) = h_{\overrightarrow{\mathcal{X}}}(\mathcal{P}_1, \mathcal{P}_2)$, $d_\mathcal{P}(\mathcal{T}_1, \mathcal{T}_2) = h_\mathcal{X}(\mathcal{P}_1, \mathcal{P}_2)$. A consequence of the properties of the Hausdorff distance is the following: $d_{\overrightarrow{\mathcal{P}}}(\mathcal{T}_1, \mathcal{T}_2) = 0 \Leftrightarrow cl(\mathcal{P}_1) \subseteq cl(\mathcal{P}_2)$, $d_\mathcal{P}(\mathcal{T}_1, \mathcal{T}_2) = 0 \Leftrightarrow cl(\mathcal{P}_1) = cl(\mathcal{P}_2)$. We use the definition of approximate simulation and bisimulation relations proposed by Julius and Pappas in [18]. Let $\mathcal{T}_1 = (Q_1, Q_0^1, \Sigma_1, E_1, \Omega_1, \omega_1)$ and $\mathcal{T}_2 = (Q_2, Q_0^2, \Sigma_2, E_2, \Omega_2, \omega_2)$ be two labeled metric transition systems such that $\Sigma_1 = \Sigma_2 = \Sigma$ and $\Omega_1 = \Omega_2 = \Omega$.

Definition 2 (Approximate simulation relation): [18] A relation $\Gamma \subseteq Q_1 \times Q_2$ is called a (ε, δ) approximate simulation relation of $\mathcal{T}_1$ by $\mathcal{T}_2$, if for all $(q_1, q_2) \in \Gamma$:

1) $d_\Omega(\omega_1(q_1), \omega_2(q_2)) \leq \delta$,
2) for all $q_1 \overset{\sigma}{\to} q_1'$, there exists $q_2 \overset{\sigma'}{\to} q_2'$ such that $(q_1', q_2') \in \Gamma, d_\Sigma(\sigma, \sigma') \leq \varepsilon$.

Definition 3 (Approximate bisimulation relation): Given $\mathcal{T}_1$ by $\mathcal{T}_2$, a relation Γ is called a (ε, δ) approximate bisimulation relation when it is both a (ε, δ) approximate simulation relation of $\mathcal{T}_1$ by $\mathcal{T}_2$, and a (ε, δ) approximate simulation relation of $\mathcal{T}_2$ by $\mathcal{T}_1$.

Definition 4 (Approximate simulation): [18] $\mathcal{T}_2$ is a (ε, δ) approximate simulation of $\mathcal{T}_1$ (denoted $\mathcal{T}_1 \preceq_{(\varepsilon,\delta)} \mathcal{T}_2$) if there exists Γ, a (ε, δ) approximate simulation relation of $\mathcal{T}_1$ by $\mathcal{T}_2$, such that for all $q_1 \in Q_0^1$, there exists $q_2 \in Q_0^2$ such that $(q_1, q_2) \in \Gamma$.

Definition 5 (Approximate bisimulation): Given $\mathcal{T}_1$ by $\mathcal{T}_2$, if $\mathcal{T}_1 \preceq_{(\varepsilon,\delta)} \mathcal{T}_2$ and $\mathcal{T}_2 \preceq_{(\varepsilon,\delta)} \mathcal{T}_1$, then we say that $\mathcal{T}_1$ and $\mathcal{T}_2$ are approximately bisimilar with precision (ε, δ), and write $\mathcal{T}_1 \approx_{(\varepsilon,\delta)} \mathcal{T}_2$.

We define a simulation metric, as the tightest precision (ε, δ) (we use element-wise inequality as partial ordering relation of pairs (ε, δ)) such that $\mathcal{T}_1 \preceq_{(\varepsilon,\delta)} \mathcal{T}_2$: $d_{\overrightarrow{\mathcal{S}}}(\mathcal{T}_1, \mathcal{T}_2) = \inf\{(\varepsilon, \delta) : \mathcal{T}_1 \preceq_{(\varepsilon,\delta)} \mathcal{T}_2\}$. We can also define a bisimulation metric, as the tightest precision (ε, δ) such that $\mathcal{T}_1 \approx_{(\varepsilon,\delta)} \mathcal{T}_2$: $d_\mathcal{B}(\mathcal{T}_1, \mathcal{T}_2) = \inf\{\varepsilon : \mathcal{T}_1 \approx_{(\varepsilon,\delta)} \mathcal{T}_2\}$. The following diagram summarizes the classical relations between language and simulation metrics:

$$\begin{array}{ccc} d_\mathcal{B}(\mathcal{T}_1, \mathcal{T}_2) & \geq & d_\mathcal{P}(\mathcal{T}_1, \mathcal{T}_2) \\ \geq & & \geq \\ d_{\overrightarrow{\mathcal{S}}}(\mathcal{T}_1, \mathcal{T}_2) & \geq & d_{\overrightarrow{\mathcal{P}}}(\mathcal{T}_1, \mathcal{T}_2) \end{array}$$

If the transition systems are deterministic, then the following classical result holds:

$$d_{\overrightarrow{\mathcal{S}}}(\mathcal{T}_1, \mathcal{T}_2) = d_{\overrightarrow{\mathcal{P}}}(\mathcal{T}_1, \mathcal{T}_2), \quad d_\mathcal{B}(\mathcal{T}_1, \mathcal{T}_2) = d_\mathcal{P}(\mathcal{T}_1, \mathcal{T}_2)$$

We will state the theoretical results of this paper in the framework of transition systems. However, we specialize some definitions in order to use transition systems as a unifying mathematical framework to model hybrid automata (and thus timed automata, that is a subclass of hybrid automata), according to the classical embedding of hybrid automata into transition systems (see e.g. [12]). The state set Q of the transition system is given by the cartesian product of the continuous and the discrete state space. The set of labels $\Sigma = \mathbb{R}_+ \cup \{0\} \times \Psi \cup \{\varepsilon\}$ models a continuous time duration $\Delta \in \mathbb{R}_+ \cup \{0\}$ and a discrete output symbol $\psi \in \Psi$, which can also be an unobservable output ε. The set Ω models the set of discrete states. In this setting, a transition $(q, x) \overset{\Delta,\psi}{\to} (q', x')$ is associated to a trajectory $q \overset{\Delta,\psi}{\to} q'$, and models that the discrete state q' can be reached from the discrete state q in time Δ and with observation ψ. We define the minimum dwell time Δ_m as the minimum time that can be spent in a discrete state. This implies that given any transition $(q, x) \overset{\Delta,\psi}{\to} (q', x'), q \neq q'$, then $\Delta \geq \Delta_m$. We will assume in the rest of the paper that $\Delta_m > 0$, namely two successive discrete transitions can not occur at the same time instant.

Because of unobservable outputs, the external trajectory $P(\rho) = \Delta_1, \psi_1, \cdots, \Delta_{|\rho|}, \psi_{|\rho|}$ is redefined by erasing all unobservable outputs $\psi_i = \varepsilon$, and by adding up the adjacent time delays $\Delta_i + \Delta_{i+1}$. This implies that $|P(\rho)| \leq |\rho|$. For instance, the external trajectory $3, \psi_1, 4, \varepsilon, 5, \psi_2, 2, \psi_3$ is redefined as $3, \psi_1, 9, \psi_2, 2, \psi_3$. Given external trajectories

$p_1 = \{\Delta_i^1, \psi_i^1\}_{i=1}^{|p_1|}$, $p_2 = \{\Delta_i^2, \psi_i^2\}_{i=1}^{|p_2|} \in \mathcal{X}(\Sigma)$, we define the undirected distance $d_{\mathcal{X}}$:

$$d_{\mathcal{X}}(p_1, p_2) = \begin{cases} \sup\limits_i d_{\mathcal{E}}\left(\Delta_i^1, \Delta_i^2\right) \\ \text{if } |p_1| = |p_2| \text{ and } \forall i = 1 \cdots |p_1|, \psi_i^1 = \psi_i^2 \\ \\ +\infty \text{ otherwise} \end{cases} \tag{1}$$

where $d_{\mathcal{E}}$ is the Euclidean metric. This metric defines the distance between two external trajectories with the same sequence of discrete outputs, as the maximum duration difference of two discrete transitions associated to the same index. We will introduce in the next section a general diagnosability definition, that leverages on the metric $d_{\mathcal{X}}$ to take into account the measurements uncertainty of the time duration between two discrete outputs.

III. Diagnosability definition

Given a transition system $\mathcal{T}$, let $\Omega_c \subset \Omega$ be a set of states that model a failure in $\mathcal{T}$: Ω_c is called *faulty set*. A *δ–faulty trajectory* is a trajectory that enters the faulty set at a certain time instant, and then continues flowing for a time duration δ.

Definition 6 (δ–faulty trajectory): A trajectory

$$\rho = \omega(q_0) \overset{\Delta_1, \psi_1}{\rightarrow} \omega(q_1) \cdots \overset{\Delta_{|\rho|}, \psi_{|\rho|}}{\rightarrow} \omega(q_{|\rho|}) \in \mathcal{L}$$

is δ–faulty if there exists a finite index $k_c \geq 0$, $k_c \leq |\rho|$ if $|\rho| < \infty$, such that $\forall k < k_c, \omega(q_k) \notin \Omega_c$, $\omega(q_{k_c}) \in \Omega_c$, $\sum\limits_{k=k_c+1}^{|\rho|} \Delta_k = \delta$.

We define $\mathcal{F}_\delta$ the set of all δ–faulty trajectories, and $\mathcal{F} = \bigcup\limits_{\delta \geq 0} \mathcal{F}_\delta \subseteq \mathcal{L}$ the set of all faulty trajectories.

We propose a diagnosability notion, that depends on two parameters $(\delta_d, \delta_m) \in \mathbb{R}_+ \cup \{0\} \times \mathbb{R}_+ \cup \{0\}$. The first parameter specifies that if a trajectory has visited the faulty set, this can be detected only using the external trajectory within a delay upper bounded by δ_d. The second parameter specifies the available precision δ_m when measuring time delays of the external trajectory. In other words, for any given external trajectory $p = \Delta_1, \psi_1, \cdots, \Delta_{|p|}, \psi_{|p|}$ the corresponding measured observation is $\hat{p} = \hat{\Delta}_1, \psi_1, \cdots, \hat{\Delta}_{|p|}, \psi_{|p|}$, where $\forall i = 1 \cdots |p|, \hat{\Delta}_i \in [\Delta_i - \delta_m, \Delta_i + \delta_m]$. This is reasonable, since a time counter is always affected by a measurement error. When a new output symbol ψ_i is generated, the counter provides the measure $\hat{\Delta}_i, \psi_i$, and resets to measure the next duration $\hat{\Delta}_{i+1}$ up to the generation of ψ_{i+1}. The metric $d_{\mathcal{X}}$ has been defined with the purpose of considering the measurement error described above, and can be used to state necessary and sufficient diagnosability conditions.

Definition 7 ((δ_d, δ_m)-diagnosability): A pair $(\mathcal{T}, \Omega_c)$ is (δ_d, δ_m)–diagnosable if and only if

$$\forall \rho \in \bigcup_{\delta \geq \delta_d} \mathcal{F}_\delta, \ \forall \rho' \in \mathcal{L} \setminus \mathcal{F}, \ d_{\mathcal{X}}\left(P(\rho), P(\rho')\right) \leq \delta_m$$

When the measurement error is zero, i.e. $\delta_m = 0$, the notion of $(\delta_d, 0)$–diagnosability coincides with δ_d–diagnosability as defined in [8]. If Ω_c models a set $\{\Omega_1, \cdots, \Omega_F\}$ of faults such that $\Omega_c = \bigcup\limits_{i=1}^{F} \Omega_i$, and we want to require that it is possible to identify which fault has occurred, then we just need to check whether $(\mathcal{T}, \Omega_i)$ is (δ_d, δ_m)–diagnosable for each $i = 1, \cdots, F$. That is, our diagnosability definition allows to express both fault detection and fault isolation properties.

Proposition 1: Given $\mathcal{T}$ and Ω_c, the following statements hold:

1) If $(\mathcal{T}, \Omega_c)$ is (δ_d, δ_m)–diagnosable, then it is (δ_d^*, δ_m)–diagnosable for all $\delta_d^* \geq \delta_d$.
2) If $(\mathcal{T}, \Omega_c)$ is not (δ_d, δ_m)–diagnosable, then it is not (δ_d^*, δ_m)–diagnosable for all $\delta_d^* \leq \delta_d$.
3) If $(\mathcal{T}, \Omega_c)$ is (δ_d, δ_m)–diagnosable, then it is (δ_d, δ_m^*)–diagnosable for all $\delta_m^* \leq \delta_m$.
4) If $(\mathcal{T}, \Omega_c)$ is not (δ_d, δ_m)–diagnosable, then it is not (δ_d, δ_m^*)–diagnosable for all $\delta_m^* \geq \delta_m$.

The proposition above shows two interesting properties. By a verification point of view, given an available measurement precision δ_m, it is interesting to compute the minimum value δ_d^{min} (the delay needed in order to perform a fault detection) for which $(\mathcal{T}, \Omega_c)$ is $(\delta_d^{min}, \delta_m)$–diagnosable. By a design point of view, given a required maximum delay δ_d for fault detection, it is interesting to compute the maximum value δ_m^{max} (the coarsest measurement precision needed) for which $(\mathcal{T}, \Omega_c)$ is $(\delta_d, \delta_m^{max})$–diagnosable.

IV. Verification by abstraction

Given two transition systems $\mathcal{T}_1, \mathcal{T}_2$ that are approximately bisimilar with precision ε according to the metric $d_{\mathcal{X}}$, we state in this section a relation between (δ_d, δ_m)–diagnosability of the two systems. According to the metric $d_{\mathcal{X}}$, the timed trajectories of $\mathcal{T}_1$ and $\mathcal{T}_2$ diverge as the number of transitions goes to infinity, since each transition introduces a finite error. This issue introduces technical problems when relating diagnosability of $\mathcal{T}_1$ and $\mathcal{T}_2$. We show that, using a diagnosability definition that is also related to a measurement uncertainty δ_m, it is possible to compare (δ_d, δ_m)–diagnosability of $\mathcal{T}_1$ and $\mathcal{T}_2$. We introduce the main result of this paper:

Theorem 1: Let a pair $(\mathcal{T}_2, \Omega_c^2)$ be given, and let $(\mathcal{T}_1, \Omega_c^1)$ be an abstraction that satisfies the following:

$$\mathcal{T}_1 \approx_{(\varepsilon,0)} \mathcal{T}_2, \tag{2}$$

$$(q_1, q_2) \in \Gamma \Rightarrow (q_1 \in \Omega_c^1 \wedge q_2 \in \Omega_c^2) \vee (q_1 \notin \Omega_c^1 \wedge q_2 \notin \Omega_c^2). \tag{3}$$

where Γ is the $(\varepsilon, 0)$ approximate bisimulation relation for $\mathcal{T}_1, \mathcal{T}_2$. Then the following hold:

1) If $(\mathcal{T}_1, \Omega_c^1)$ is not (δ_d, δ_m)–diagnosable, then $(\mathcal{T}_2, \Omega_c^2)$ is not $\left(\delta_d\left(1 - \frac{\varepsilon}{\Delta_m}\right), \delta_m + 2\varepsilon\right)$–diagnosable.
2) If $(\mathcal{T}_1, \Omega_c^1)$ is (δ_d, δ_m)–diagnosable, then $(\mathcal{T}_2, \Omega_c^2)$ is $\left(\delta_d\left(\frac{\Delta_m}{\Delta_m - \varepsilon}\right), \delta_m - 2\varepsilon\right)$–diagnosable.

The above theorem, given for the general class of transition systems, applies to many classes of systems, provided that they can be formalized as transitions systems (e.g. continuous and discrete time linear and non-linear systems, discrete event systems, hybrid systems, etc.). On the basis of Theorem 1, we propose a procedure to check diagnosability of a hybrid automaton on a durational graph approximate abstraction. In [11] we proposed an algorithmic procedure to obtain, for any precision ε, a durational graph abstraction $\mathcal{G}$ and a critical set $\Omega_c^{\mathcal{G}}$ of a given hybrid automaton $\mathcal{H}$ and critical set $\Omega_c^{\mathcal{H}}$ such that $\mathcal{H} \approx_{(\varepsilon,0)} \mathcal{G}$ according to the metric $d_{\mathcal{X}}$ defined in (1), and such that Condition (3) of Theorem 1 is satisfied.

Moreover, we proposed in [8] a procedure to compute in polynomial time, for a given durational graph $\mathcal{G}$, the minimum value δ_d^{min} for which $(\mathcal{G}, \Omega_c)$ is $(\delta_d^{min}, 0)$–diagnosable. This algorithm can be extended in order to compute the minimum value δ_d^{min} for which $(\mathcal{G}, \Omega_c)$ is $(\delta_d^{min}, \delta_m)$–diagnosable for any given δ_m.

In fact, the algorithm introduced in [8] exploits properties of product automata composition to generate the language of pairs of executions $\rho \in \mathcal{F}, \rho' \in \mathcal{L} \setminus \mathcal{F}$ that produce the same observation $P(\rho) = P(\rho')$. The exact product automata composition operator $||$ is illustrated at the top of Figure 1: given two states q_1, q_2, and two edges $e_1 = (q_1, q_1'), e_2 = (q_2, q_2')$ associated to transition time sets G_1, G_2, they synchronize in the exact product automaton if and only if $G_1 \cap G_2 \neq \varnothing$, generating state $q = (q_1, q_2), q' = (q_1', q_2')$, and an edge $e = ((q_1, q_2), (q_1', q_2'))$ associated to transition time set $G = G_1 \cap G_2$.

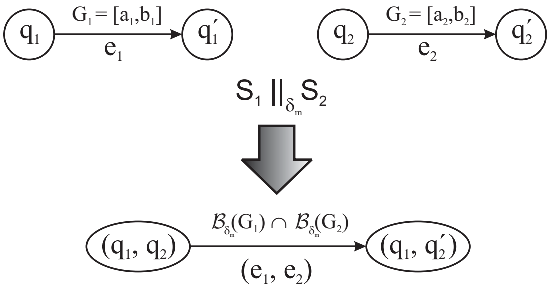

Fig. 1. Exact and approximate product automata composition operators.

The δ_m approximate product automata composition operator $||_{\delta_m}$ is illustrated at the bottom of Figure 1: given two states q_1, q_2, two edges $e_1 = (q_1, q_1'), e_2 = (q_2, q_2')$ associated to transition time sets G_1, G_2 synchronize in the δ_m approximate product automaton if and only if $\mathcal{B}_{\delta_m}(G_1) \cap \mathcal{B}_{\delta_m}(G_2) \neq \varnothing$, generating a state $q = (q_1, q_2)$, and an edge $e = ((q_1, q_2), (q_1', q_2'))$ associated to transition time set $G = \mathcal{B}_{\delta_m}(G_1) \cap \mathcal{B}_{\delta_m}(G_2)$. Using δ_m approximate product automata composition in the algorithm proposed in [8], one generates the language of pairs of executions $\rho \in \mathcal{F}, \rho' \in \mathcal{L} \setminus \mathcal{F}$ that generate δ_m close observations $d_{\mathcal{X}}(P(\rho), P(\rho')) \leq \delta_m$, and thus compute δ_d^{min}.

Let a hybrid automaton $\mathcal{H}$ be given, and let $\mathcal{G}$ be a durational graph abstraction such that $\mathcal{H} \approx_{(\varepsilon,0)} \mathcal{G}$. For the reasons above, given $\mathcal{G}$ and δ_m, it is possible to compute, in polynomial time with respect to the cardinality of the state space of a durational graph, the minimum value δ_d^{min} for which $(\mathcal{G}, \Omega_c)$ is $(\delta_d^{min}, \delta_m)$–diagnosable. Since δ_d^{min} can be either a minimum or an inferior bound, we assume without loss of generality that it is a minimum value. The following hold by Proposition 1:

- $(\mathcal{G}, \Omega_c^{\mathcal{G}})$ is (δ_d, δ_m)–diagnosable for any $\delta_d \geq \delta_d^{min}$;
- $(\mathcal{G}, \Omega_c^{\mathcal{G}})$ is not (δ_d, δ_m)–diagnosable for any $\delta_d < \delta_d^{min}$.

Theorem 1 implies the following:

- $(\mathcal{H}, \Omega_c^{\mathcal{H}})$ is $(\delta_d, \delta_m - 2\varepsilon)$–diagnosable for any $\delta_d \geq \delta_d^{min}\left(\frac{\Delta_m}{\Delta_m - \varepsilon}\right)$;
- $(\mathcal{H}, \Omega_c^{\mathcal{H}})$ is not $(\delta_d, \delta_m + 2\varepsilon)$–diagnosable for any $\delta_d < \delta_d^{min}\left(1 - \frac{\varepsilon}{\Delta_m}\right)$.

This implies that the minimum value $\bar{\delta}_d^{min}$ for which $(\mathcal{H}, \Omega_c^{\mathcal{H}})$ is $(\bar{\delta}_d^{min}, \bar{\delta}_m)$–diagnosable belongs to the interval $\left[\delta_d^{min}\left(1 - \frac{\varepsilon}{\Delta_m}\right), \delta_d^{min}\left(\frac{\Delta_m}{\Delta_m - \varepsilon}\right)\right]$, and $\bar{\delta}_m$ belongs to the interval $[\delta_m - 2\varepsilon, \delta_m + 2\varepsilon]$.

Notice that, without defining diagnosability also with respect to the measurement error δ_m, there does not exist a relation between diagnosability of the approximately bisimilar systems. In fact, for any fixed $\varepsilon > 0, \delta_m$, and if the abstraction is (δ_d, δ_m)-diagnosable, it is not possible to infer (δ_d^*, δ_m^*)-diagnosability of the original system with $\delta_m^* = \delta_m$. However, it is possible to relate δ_m^* to a boundary of δ_m, and this is not possible without our diagnosability definition also given with respect to the measurement precision.

V. Case Study

Camless electromagnetic valves are interesting devices which can be used to command the opening and closing phases of the intake and exhaust valves in an internal combustion engine. Since they decouple the camshaft and the valve lift dynamics, they may obtain the optimal engine efficiency in all operating conditions. An open problem is the control of the impact velocities between the valve and the constraints, which should be sufficiently low in order to eliminate acoustic noises and avoid damages of the mechanical components. The problem is complicated by the short travel time to make a transition between the two valve's terminal positions. At high engine speed this time is $\sim 10^{-3}$ s. We consider a simplified model of the electromagnetic valve (see [1], [9], [10] and references therein for details). We suppose here to supply only one electromagnet to complete the opening or closing phase. The correct behavior of the valve controlled system can be modeled by the hybrid automaton $\mathcal{H}^1$ shown in Figure 2: q_1 corresponds to the closing phase, q_2 to the valve completely close, q_3 to the opening phase, and q_4 to the valve completely open. The continuous dynamics can be described by the following equations:

$$\dot{x}_v = v_v, \ \dot{v}_v = \frac{1}{M}\Big(-kx_v - bv_v + F_m + F_d + F_c\Big) \quad (4)$$

describing the motion of the valve and of the connected anchor, where M is the mass. The valve position x_v ranges from $-\rho$ (open valve) to $+\rho$ (closed valve). Moreover, an elastic force $-kx_v$, due to some springs and a torsion bar, and a viscous friction $-b\dot{x}_v$ act on the valve steam. Finally, F_d is a disturbance whose main contribution is due to the force of the exhaust gases exiting the cylinder, and $F_c(x_v)$ is the constrain force due to the valve seat and electromagnet surfaces, and is always zero except when $x_v = \pm\rho$, when $F_c(\pm\rho) = \pm k\rho - F_m(\pm\rho, \phi_m) - F_d$. The anchor is attracted by the supplied electromagnet to close and to open the valve by means of the electromagnet force

$$F_m(x_v, \phi_m) = -\frac{1}{2}\mathcal{D}_m(x_v)\phi_m^2, \quad \mathcal{D}_m = a_m e^{-b_m x_v} + c_m, \quad (5)$$

where a_m, b_m, c_m are some constants, and ϕ_m is the flux of the supplied electromagnet $m = 1, 2$. The dynamics of ϕ_m is here neglected for simplicity, since they are much faster than the mechanical ones, so that the squared flux can be considered as the control input of the system, i.e. $u = \phi_m^2$. The signs of the constants are such that $\mathcal{D}_1(x_v) > 0$ for the discrete states q_1, q_2, namely when the valve is closing and the electromagnet 1 is supplied, while $\mathcal{D}_2(x_v) < 0$ for the discrete states q_3, q_4, namely when the valve is opening and the electromagnet 2 is supplied. The discrete dynamics depend on the system state (x_v, v_v) and the control input u, according to the guard sets (defined on arrows in Figure 2) and invariant sets (associated to the discrete states in Figure 2). The reset functions are all identities. Without loss of generality, we assume that the initial hybrid state is $(q_1, (-\rho, 0))$, but our results can be easily extended to more complex sets of initial states. The output of the system is a discrete symbol associated to the edges, i.e. ψ_1 or ψ_2 when the anchor hits respectively electromagnet 1 or electromagnet 2. It follows from [9], [1] that the PD–like control

$$u = \frac{2}{\mathcal{D}_m(x_v)}\Big(p_1(x_v - x_r) + p_2(v_v - v_r) + F_d - kx_r - bv_r - Ma_r\Big)$$

$p_1, p_2 > 0$ ensures the correct behavior of the valve. Here $x_r = (-1)^{m+1}\rho$, $m = 1, 2$, $v_r = 0$, $a_r = 0$ are the reference values for appropriately operating the valve.

Following [10] and setting $e = \begin{pmatrix} x_v - x_r & v_v - v_r \end{pmatrix}^T$, when $F_c = 0$ and using the above control, the error dynamics are given by $\dot{e} = A_c e$, where

$$A_c = \begin{pmatrix} 0 & 1 \\ -k_1 & -b_1 \end{pmatrix}, \qquad \begin{aligned} k_1 &= \frac{k + p_1}{M} > 0, \\ b_1 &= \frac{b + p_2}{M} > 0. \end{aligned} \tag{6}$$

In this work we are interested to investigate if, for this electromagnetic valve, it is possible to assess the diagnosability property introduced in the previous sections. Differently from what done in [8], we consider uncertainty in the system parameters, and not in the controller parameters. For, we assume that the system parameters k, b are subject to abrupt changes, due to possible malfunctions. Let k_0, b_0 be their nominal values and $k = k_0 + \Delta k$, $b = b_0 + \Delta b$ the real ones. The controller parameters (p_1, p_2) must be chosen to satisfy the following constraints for the nominal values $k = k_0$ and $b = b_0$.

1) The tracking error goes asymptotically to zero;
2) The norm of the control input is bounded by $u_{\max}$;
3) The seating velocity, i.e. the velocity of the valve when approaching the mechanical constraints, is less than or equal to an appropriate value $v_{\max}$.

From the first assumption we obtain $p_1 > -k$, $p_2 > -b$. Setting $F_{d,\max} = \max_{t \ge 0} F_d(t)$ and $e_{v,\max}$ the maximum velocity error admissible, from the second we obtain

$$|u| \le \frac{2}{\min_{x_v} \mathcal{D}_m(x_v)}\Big(p_1 2\rho + p_2 e_{v,\max} + F_{d,\max} + k\rho\Big) \le u_{\max}. \tag{7}$$

Since $2(F_{d,\max} + k\rho)/\min_{x_v} \mathcal{D}_m(x_v) - u_{\max} \simeq -u_{\max} = -a_3$, (7) can be approximated by

$$a_1 p_1 + a_2 p_2 - a_3 + a_0 k \simeq a_1 p_1 + a_2 p_2 - a_3 \le 0 \tag{8}$$

with $a_0 = 8 \times 10^{-11}$, $a_1 = 1.6 \times 10^{-10}$, $a_2 = 2 \times 10^{-7}$, $a_3 \simeq 1 \times 10^6$, see Table I. For the third assumption, note that the raising time for the error dynamics is $t_r = \pi/\sqrt{4k_1 - b_1^2}$, where $4k_1 - b_1^2 > 0$ to obtain a fast response, namely

$$p_1 > \frac{1}{4M}\big(b + p_2\big)^2 - k. \tag{9}$$

TABLE I

ELECTROMAGNETIC VALVE SYSTEM PARAMETERS

$k_0 = 1.17 \times 10^5$ N/m	$b_0 = 6$ Ns/m	$M = 0.1054$ Kg
$F_{d,\max} = 3410$ N	$\rho = 4 \times 10^{-3}$ m	$e_{v,\max} = 10$ m/s
$\min_{x_v} \mathcal{D}(x_v) = 1 \times 10^8$	$u_{\max} = 1 \times 10^6$ V	$v_{\max} = 0.05$ m/s

Hence, the velocity error has to satisfy $|v_v - v_r|_{t=t_r} = 2\rho e^{-\frac{b_1}{2}t_r} \le v_{\max}$, thus obtaining

$$\begin{aligned} p_1 &\le \frac{1}{4M}\frac{1+n^2}{n^2}\big(b + p_2\big)^2 - k \quad \text{if } n = \frac{2}{\pi}\ln\frac{2\rho}{v_{\max}} \ge 0 \\ p_2 &> b_2 \quad \text{if } n < 0. \end{aligned} \tag{10}$$

A solution to (9), (10) exists since $1 + n^2/n^2 > 1$. Conditions (8), (9), (10) for $k = k_0$, $b = b_0$ define the set of controller parameters ensuring the correct behavior. A pair in this set is for instance $(p_1^*, p_2^*) = (1.17 \times 10^4, 0.6)$, which corresponds to a travel time for the anchor of $\simeq 1.45$ ms.

We assume that Δk can vary in the interval $\mathcal{I}_k = [-k_0, k_0]$, where $-k_0$ corresponds to $k = 0$ (the spring is broken). Moreover, we assume that Δb can vary in the interval $\mathcal{I}_b = [-0.9b_0, 2b_0]$: in other words, the viscous friction can increase up to 200% of the nominal value, and can decrease up to 90% of the nominal value. We define $P = [-k_0, k_0] \times [-0.9b_0, 2b_0]$.

When (k, b) changes, the controller may not ensure the correct valve behavior. In fact, the variations Δk, Δb may exit the safe set $P_{safe} \subset P$, and a faulty behavior may occur. In order to determine P_{safe}, let us set $p_1 = p_1^*, p_2 = p_2^*$ in (8), (9), (10), with $k = k_0 + \Delta k$, $b = b_0 + \Delta b$:

$$\begin{aligned} \Delta k &\le \frac{a_3 - p_1^* a_1 - p_2^* a_2 - a_0 k_0}{a_0} \simeq \frac{a_3 - p_1^* a_1 - p_2^* a_2}{a_0} \\ \Delta k &> \frac{1}{4M}\big(b_0 + \Delta b + p_2^*\big)^2 - p_1^* - k_0 \\ \Delta k &\le \frac{1}{4M}\frac{1+n^2}{n^2}\big(b_0 + \Delta b + p_2^*\big)^2 - p_1^* - k_0. \end{aligned}$$

We assume that $(\Delta k, \Delta b)$ may abruptly belong to a faulty value in the set

$$P_{faulty} \triangleq [-1.17 \times 10^5, -0.8075 \times 10^5) \times [-5.4, 12].$$

In this case, the corresponding dynamics of the controlled system switch to the *faulty dynamics*, modeled in Figure 2 by the hybrid automaton $\mathcal{H}^2$. The dynamics of each discrete state of $\mathcal{H}^2$ is the same as in $\mathcal{H}^1$, except for the value of the parameters k, b. The sudden change of the system parameters to a faulty value may occur at any time instant from discrete states q_1, q_3, and we assume that is associated to an unobservable output. The overall model $\mathcal{H}$ takes into account fault occurrence as illustrated in Figure 2: we assume that the system does not return to a correct behavior once it switches to a faulty behavior. Since the guards are 1–dimensional and the dynamics are linear, we can construct a durational graph abstraction $\mathcal{G}$, such that $\mathcal{H} \approx_{(\varepsilon,0)} \mathcal{G}$ for any desired $\varepsilon > 0$.

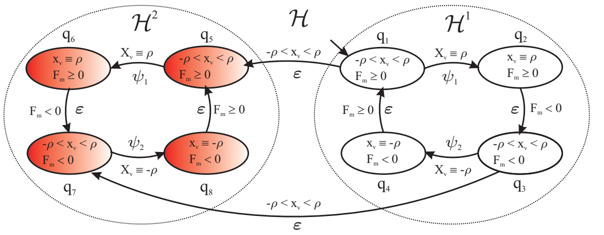

Fig. 2. Hybrid model of the Electromagnetic Valve System $\mathcal{H}$.

In order to compute such $\mathcal{G}$, the sets $\mathcal{I}_k$, $\mathcal{I}_b$ are partitioned in n, m subintervals of width $\delta_k = 2k_0/n, \delta_b = 2.9\, b_0/m$. Considering $\delta_k = 0.39 \times 10^5$, $\delta_b = 2.9$ one gets 6 faulty sets and 33 safe sets. To each element of these partition corresponds 4 discrete states of the abstraction $\mathcal{G}$. The discrete state space of $\mathcal{G}$ consists of 156 discrete states. We compute the minimum and maximum time for the anchor to touch electromagnet 1 starting from electromagnet 2 and viceversa, for each element of the partition that belongs to the faulty and non faulty set. Because of the geometry of the partition elements, for each of the 6 faulty sets and 33 safe sets, it is possible to compute exactly the minimum and maximum travel times for the anchor. Applying the diagnosability verification algorithm developed in [8], and using the approximate composition introduced in the above section, one can verify that the minimum value δ_d^{min} and the maximum value δ_m^{max} such that $\mathcal{G}$ is $(\delta_d^{min}, \delta_m^{max})$–diagnosable are given by $\delta_d^{min} = 4.7\,\mathrm{ms}$, $\delta_m^{max} = 0.06\,\mathrm{ms}$. Moreover, because of the special dynamics and structure of guards (switching times can be computed exactly) and resets (the resets are memoryless, namely they do not depend on the continuous state) of the hybrid model, it is easy to verify that, for any partition of the faulty and safe parameter sets, diagnosability conditions on $\mathcal{G}$ are the same for any precision $\varepsilon \geq 0$ such that $\mathcal{H} \approx_{(\varepsilon,0)} \mathcal{G}$. Thus, we can apply the result of Theorem 1 for $\varepsilon = 0$, and state that the minimum value δ_d^{min} and the maximum value δ_m^{max} such that $\mathcal{H}$ is $(\delta_d^{min}, \delta_m^{max})$–diagnosable are $\delta_d^{min} = 4.7\,\mathrm{ms}, \delta_m^{max} = 0.06\,\mathrm{ms}$. Namely, if we consider P_{faulty} as the set of faulty behaviors, then we can detect whether the system parameters enter the set P_{faulty} within $4.7\,\mathrm{ms}$, by using measurements affected by an error bounded by $0.06\,\mathrm{ms}$.

VI. Conclusions

We proposed a novel diagnosability notion, i.e. (δ_d, δ_m)-diagnosability, that also depends on the measurements uncertainty δ_m. Given an approximate abstraction T_1 of a system T_2 with precision ε, we derived a relation between diagnosability properties of T_1 and T_2 as a function of $\delta_d, \delta_m, \varepsilon$. We have shown that deriving such a relation is not possible using the previous diagnosability definition, i.e. δ_d-diagnosability. We applied our results to an electromagnetic valve system for cam-less engines.

References

[1] C. Acosta Lua, B. Castillo Toledo, M. D. Di Benedetto, and S. Di Gennaro. Nonlinear control of electromagnetic valves for camless engines. Technical report, Department of Electrical and Computer Science, University of L'Aquila, 2006. http://www.diel.univaq.it/research/.

[2] R. Alur, C. Courcoubetis, N. Halbwachs, T.A. Henzinger, P.H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138:3–34, 1995.

[3] R. Alur, T. Henzinger, G. Lafferriere, and G. Pappas. Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88(2):971–984, July 2000.

[4] Paul Caspi and Albert Benveniste. Toward an approximation theory for computerised control. In *Proceedings of the 2^{nd} International Workshop on Embedded Software, EMSOFT2002, Grenoble*, page Volume 2491 in Lecture Notes in Computer Science, October 2002.

[5] E.M. Clarke, O. Grumberg, and D.A. Peled. *Model Checking*. The MIT Press, Cambridge, Massachusetts, 2002.

[6] M. D. Di Benedetto, S. Di Gennaro, and A. D'Innocenzo. Error detection within a specific time horizon and application to air traffic management. In *Proceedings of the Joint 44^{th} IEEE Conference on Decision and Control and European Control Conference (CDC-ECC'05), Seville, Spain*, pages 7472–7477, December 2005.

[7] M. D. Di Benedetto, S. Di Gennaro, and A. D'Innocenzo. Critical states detection with bounded probability of false alarm and application to air traffic management. In *Proceedings of the 2^{nd} IFAC Conference on Analysis and Design of Hybrid Systems (ADHS), Alghero, Sardinia, Italy*, June 7-9 2006.

[8] M.D. Di Benedetto, S. Di Gennaro, and A. D'Innocenzo. Diagnosability verification for hybrid automata and durational graphs. In *Proceedings of the 46^{th} IEEE Conference on Decision and Control. New Orleans, Louisiana, USA.*, 12-14 December 2007.

[9] S. Di Gennaro, B. Castillo Toledo, and M. D. Di Benedetto. Nonlinear regulation of electromagnetic valves for camless engines. In *Proceedings of the 45^{th} IEEE Conference on Decision and Control, San Diego, CA, USA*, 13-15 December 2006.

[10] S. Di Gennaro, B. Castillo Toledo, and M. D. Di Benedetto. Nonlinear control of electromagnetic valves for camless engines. *International Journal of Control,* Special Issue on Automotive Control, 80 (11):1796–1813, 2007.

[11] A. D'Innocenzo, A.A. Julius, M.D. Di Benedetto, and G.J. Pappas. Approximate timed abstractions of hybrid automata. In *Proceedings of the 46^{th} IEEE Conference on Decision and Control. New Orleans, Louisiana, USA.*, 12-14 December 2007.

[12] A. D'Innocenzo, A.A. Julius, G.J. Pappas, M.D. Di Benedetto, and S. Di Gennaro. Verification of temporal properties on hybrid automata by simulation relations. In *Proceedings of the 46^{th} IEEE Conference on Decision and Control. New Orleans, Louisiana, USA.*, 12-14 December 2007.

[13] D. Forstner, M. Jung, and J. Lunze. A discrete-event model of asynchronous quantised systems. *Automatica*, 38(8):1277–1286(10), August 2002.

[14] G. K. Fourlas, K. J. Kyriakopoulos, and N. J Krikelis. Diagnosability of hybrid systems. In *Proceedings of the 10th Mediterranean Conference on Control and Automation - MED2002, Lisbon, Portugal*, pages 3994–3999, July 9.12 2002.

[15] Antoine Girard and George J. Pappas. Approximation metrics for discrete and continuous systems. *IEEE Trans. on Automatic Control*, 52(5):782–798, 2007.

[16] Antoine Girard and George J. Pappas. Approximate bisimulation relations for constrained linear systems. *Automatica*, Accepted for publication.

[17] T. A. Henzinger, R. Majumdar, and V. Prabhu. Quantifying similarities between timed systems. In *Proceedings of the Third International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS)*, volume 3829 of *Lecture Notes in Computer Science*, pages 226–241. Springer, 2005.

[18] A.A. Julius and G.J. Pappas. Approximate equivalence and approximate synchronization of metric transition systems. In *Proceedings of the 45^{th} IEEE Conference on Decision and Control, San Diego, CA, USA*, December 2006.

[19] A.A. Julius and G.J. Pappas. Approximate abstraction of stochastic hybrid systems. *IEEE Trans. Automatic Control*, provisionally accepted.

[20] Feng Lin. Diagnosability of discrete event systems and its applications. *Journal of Discrete Event Dynamic Systems*, 4(2):197–212, May 2005.

[21] S. McIlraith, G. Biswas, D. Clancy, and V. Gupta. Hybrid systems diagnosis. In N. Lynch and B. Krogh, editors, *Hybrid Systems: Computation and Control*, volume 1790 of *Lecture Notes in Computer Science*, pages 282–295. Springer, 2000.

[22] A. Paoli and S. Lafortune. Safe diagnosability for fault tolerant supervision of discrete event systems. *Automatica*, 41(8), 2005.

[23] G.J. Pappas. Bisimilar linear systems. *Automatica*, 39(12):2035–2047, December 2003.

[24] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Diagnosability of discrete-event systems. *IEEE Trans. on Automatic Control*, 40(9):1555–1575, 1995.

[25] A. Sheth, C. Hartung, and R. Han. A decentralized fault diagnosis system for wireless sensor networks. In *Proceedings of the 2^{nd} IEEE International Conference on Mobile Ad-Hoc and Sensor Systems (MASS) 2005*, pages 192–194, 1999.

[26] S. Tripakis. Fault diagnosis for timed automata. *Lecture Notes in Computer Science, W. Damm and E.R. Olderog Eds., Springer Verlag*, 2469:205–221, 2002.

[27] T. Yoo and S. Lafortune. Polynomial-time verification of diagnosability of partially-observed discrete-event systems. *IEEE Trans. on automatic control*, 47(9):1491–1495, 2002.

[28] F. Zhao, X. Koutsoukos, H. Haussecker, J. Reich, and P. Cheung. Monitoring and fault diagnosis of hybrid systems. *EEE Trans. on Systems, Man, and Cybernetics I - Part B*, 35(6):1225–1240, December 2005.